대한민국특허청
KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출 원 번 호 : 10-2003-0015538
Application Number

출 원 년 월 일 : 2003년 03월 12일
Date of Application MAR 12, 2003

출 원 인 : 삼성전자주식회사
Applicant(s) SAMSUNG ELECTRONICS CO., LTD.

2003 년 09 월 23 일

특 허 청
COMMISSIONER

【서지사항】

【서류명】	특허출원서
【권리구분】	특허
【수신처】	특허청장
【제출일자】	2003.03.12
【발명의 명칭】	안전한 통신을 위한 RR 방법
【발명의 영문명칭】	RR method for secure communication
【출원인】	
【명칭】	삼성전자 주식회사
【출원인코드】	1-1998-104271-3
【대리인】	
【성명】	정홍식
【대리인코드】	9-1998-000543-3
【포괄위임등록번호】	2003-002208-1
【발명자】	
【성명의 국문표기】	이영지
【성명의 영문표기】	LEE,YOUNG JI
【주민등록번호】	771005-2231735
【우편번호】	440-807
【주소】	경기도 수원시 장안구 연무동 56-118
【국적】	KR
【심사청구】	청구
【취지】	특허법 제42조의 규정에 의한 출원, 특허법 제60조의 규정에 의한 출원심사 를 청구합니다. 대리인 정홍식 (인)
【수수료】	
【기본출원료】	17 면 29,000 원
【가산출원료】	0 면 0 원
【우선권주장료】	0 건 0 원
【심사청구료】	5 항 269,000 원
【합계】	298,000 원
【첨부서류】	1. 요약서·명세서(도면)_1통

【요약서】

【요약】

안전한 통신을 위한 RR(Return Routability) 방법이 개시된다. 본 RR 방법은, 이동노드가 홈에이전트에 HoTI 패킷을 전송하고, 대응노드에 CoTI 패킷을 전송하는 단계, 홈에이전트가 소정의 방식에 의해 생성한 제1 키 정보를 포함하는 HoTI 패킷을 대응노드에 전송하는 단계, 대응노드가 소정의 방식에 의해 생성한 제2 키 정보를 포함하는 HoT 패킷을 홈에이전트에 전송하고, 제1 키 정보로부터 소정의 방식에 의해 생성한 비밀키를 사용하여 암호화한 CoT 패킷을 이동노드에 전송하는 단계, 홈에이전트가 수신한 HoT 패킷으로부터 소정의 방식을 사용하여 생성한 비밀키를 이동노드에 전송하는 단계, 및 이동노드가 수신한 비밀키를 사용하여, 수신한 상기 암호화된 CoT 패킷을 복호화하는 단계를 구비한다. 이에 의해, 중간자 공격을 배제하여, 안정성이 향상된 RR 방법이 제공된다.

【대표도】

도 4

【색인어】

이동노드, 대응노드, 홈에이전트, RR 방법

【명세서】

【발명의 명칭】

안전한 통신을 위한 R R 방법{R R method for secure communication}

【도면의 간단한 설명】

도 1은 BU 과정을 설명하기 위한 도면,

도 2는 RR 과정을 설명하기 위한 신호 흐름도,

도 3a 내지 도 3c는 중간자 공격 과정을 설명하기 위한 도면,

도 4는 본 발명에 따른 RR 방법의 수행과정을 설명하기 위한 신호 흐름도, 그리고

도 5는 본 발명에 따른 RR 방법을 설명하기 위한 도면이다.

* 도면의 주요 부분에 대한 부호의 설명 *

100 : 이동노드 150 : 홈 에이전트

200 : 대응노드

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<9> 본 발명은 RR(Return Routability) 방법에 관한 것으로, 더욱 상세하게는 안전성을 향상시켜 안전한 통신을 보장하는 RR 방법에 관한 것이다.

<10> Mobile IPv6(Internet Protocol version 6)에서 인터넷 위의 통신 노드들은 자유롭게 링크된 네트워크를 바꾸어 가면서 통신이 가능하다. Mobile IPv6 에서, 한 링크에서 다른 링크로 자신의 접점(point of attachment)을 변화시킬 수 있는 통신 노드를 이동노드(Mobile Node

: MN) 라고 하며, 이동노드와 통신중인 대등한 노드를 대응노드(Correspond Node :CN) 라고 한다. 대응노드는 정적일 수도 있고, 동적일 수도 있다.

<11> 이동노드는 한 링크에서 다른 링크로 이동하는 경우, 자신의 홈 링크내에서 이동노드에 할당된 IP 어드레스인 홈 어드레스(Home Address)를 통해 계속 통신이 가능하다. 즉, 이동노드는 홈 링크가 아닌 외부 링크(Foreign Link)를 방문하는 동안, 이동노드와 연결된 IP 어드레스인 CoA(Care-of Address)를 할당받고, CoA를 대응노드에게 알려주어야 한다. 이에 따라, 이동노드가 자신의 홈 링크를 벗어나 다른 외부 링크로 이동하였을때 자신이 받은 CoA를 홈에이전트와 대응노드에 등록하기 BU(Binding Update) 과정이 필요하게 된다.

<12> 도 1은 BU 과정을 설명하기 위한 도면이다. 도면을 참조하면, 홈 링크에서 외부 링크로 이동한 이동노드(100)과 있고, 홈에이전트(150) 및 대응노드(200)가 있다. 홈에이전트(Home Agent)는 이동노드(100)가 자신의 현재 CoA로 등록한 홈 링크상의 라우터를 말한다.

<13> 이동노드(100)는 BU 과정을 통해, CoA를 홈에이전트(150) 및 대응노드(200)에 등록한다. BU 과정이 종료하면, 홈에이전트(150)는 이동노드(100)가 홈링크와 떨어져 있는 동안 이동노드(100)의 홈 어드레스로 예정된 홈 링크상의 패킷들을 가로채서 캡슐화한 다음, 이들은 이동노드(100)의 등록된 CoA로 터널링한다.

<14> 그런데, BU 과정을 수행하기 위해서는, 이동노드(100)가 BU 과정을 수행할 수 있는 올바른 노드인지 여부를 확인하기 위한 RR(Return Routability) 과정이 선행되어야 한다. RR 과정을 통해, 대응노드(200)가 이동노드(100)를 인증한다. 또한, RR 과정은 이동노드(100)가 BU 과정을 수행하기 위한 데이터를 홈에이전트 (150) 및 대응노드(200)에 교환하는 과정을 통해 이루어 진다.

<15> 도 2는 RR 과정을 설명하기 위한 신호 흐름도이다.

<16> 도면을 참조하며, 이동노드(100)는 홈에이전트(150)에게 HoTI(Home Test Init) 패킷을 전송하고(S300), 대응노드(200)에는 CoTI(Care of Test Init) 패킷을 전송한다(S320). 홈에이전트(150)는 이동노드(100)로부터 수신한 HoTI 패킷을 대응노드(200)에 전송한다(S310).

<17> 대응노드(200)는 HoTI 패킷과 CoTI 패킷을 수신하여 이동노드(100)를 인증하게 된다. 즉, 대응노드(200)는 HoTI 패킷에 대응하여 HoT(Home of Test) 패킷을 홈에이전트(150)에 전송하고(S330), CoTI 패킷에 대응하는 CoT(Care-of Test) 패킷을 이동노드(100)에 전송한다(S350). HoT 패킷에는 nonce 값을 포함하는 MAC 해쉬 함수가 포함되며, 이 값은 BU 과정에서 이동노드(100)를 인증하기 위해 사용된다.

<18> 그런데, 이동노드(100)와 대응노드(200)사이에는 송수신되는 패킷을 엿보는 중간자 공격(man in the middle attack)이 존재할 수 있고, 이 공격에서 공격자는 대응노드(200)에서 오는 CoT 패킷을 가로채 자신이 이동노드(100)인 것처럼 가정하거나, 또는 CoTI 패킷을 가로채서 BU의 권한을 얻는 것도 가능하다.

<19> 도 3a 내지 도 3b는 종래의 RR 과정중에 발생할 수 있는 중간자 공격의 여러가지 경우를 도시하고 있다.

<20> 도 3a의 경우는, 이동노드(100a)와 홈에이전트(150a)가 네트워크상에서 같은 라우터(50a)를 공유하고 있는 경우를 도시하고 있다. 이 경우에는, 공격자가 라우터(50a) 근처에서 HoTI 패킷 및 CoTI 패킷을 모두 가로챌 수 있다.

<21> 도 3b의 경우는, 각 노드들(100b, 150b, 200b)이 ISP(Internet service provider)(60a, 60b, 60c)를 통해 네트워크에 접속되어 있는 경우이다. 이 경우에는, 공격자가 대응노드

(200b)가 속하는 ISP(60c) 근처에서 대응노드(200b)에 전송되는 모든 패킷을 해당 ISP(60c)를 통해 가로챌 수 있다.

<22> 도 3c의 경우는, 네트워크를 통해 대응노드(200c)에게 전송되는 경로 중간에 공격자가 존재하는 경우이다. 이 경우에도, 도 3b의 경우와 마찬가지로, 대응노드 (200c)에 연결되는 경로상에 공격자가 존재하므로, 대응노드(200c)에 전송되는 모든 패킷을 가로채어 공격이 가능하게 된다.

<23> 상기한 바와 같이, 종래의 RR 과정중에는 여러가지 공격이 가능하며, 특히 공격자가 대응노드의 근처에 위치하고 있는 경우에는 대응노드에 전송되는 패킷을 가로채기가 더욱 쉬워지게 된다. 또한, Mobile IPv6의 모든 통신은 기본적으로 무선을 통해 수행되므로, 유선 통신환경에 비해 보다 많은 공격자 위협이 발생하게 된다. 따라서, RR 과정중에 중간자 공격을 방지하여, 안정성을 향상시킬 수 있는 새로운 RR 방법이 필요하게 된다.

【발명이 이루고자 하는 기술적 과제】

<24> 본 발명은 상기와 같은 문제점을 해결하기 위하여 안출된 것으로서, 본 발명의 목적은, 중간자 공격의 위협을 감소시켜, 안정성을 향상시킨 RR 방법을 제공함에 있다.

【발명의 구성 및 작용】

<25> 상기 목적을 달성하기 위한 본 발명에 따른 이동노드, 홈에이전트, 및 대응노드간의 RR(Return Routability) 방법에 있어서, 상기 이동노드가 상기 홈에이전트에 HoTI 패킷을 전송하고, 상기 대응노드에 CoTI 패킷을 전송하는 단계, 홈에이전트가 소정의 방식에 의해 생성한 제1 키 정보를 포함하는 HoTI 패킷을 상기 대응노드에 전송하는 단계, 상기 대응노드가 상기 소정의 방식에 의해 생성한 제2 키 정보를 포함하는 HoT 패킷을 상기 홈에이전트에 전송하고,

상기 제1 키 정보로부터 상기 소정의 방식에 의해 생성한 비밀키를 사용하여 암호화한 CoT 패킷을 상기 이동노드에 전송하는 단계, 상기 홈에이전트가 수신한 상기 HoT 패킷으로부터 상기 소정의 방식을 사용하여 생성한 상기 비밀키를 상기 이동노드에 전송하는 단계, 및 상기 이동노드가 수신한 상기 비밀키를 사용하여, 수신한 상기 암호화된 CoT 패킷을 복호화하는 단계를 포함한다.

<26> 상기 소정의 방식은, 공개된 파라미터 및 임의의 비밀키를 사용하는 Diffie-Hallman 키 교환 방식을 사용하는 것이 바람직하다.

<27> 또한, 상기 제1 키 정보는, 상기 HoTI 패킷의 모바일 옵셥(Mobile Options) 필드에 첨가되며, 상기 제2 키 정보는, 상기 HoT 패킷의 모바일 옵셥(Mobile Options) 필드에 첨가되는 것이 바람직하다.

<28> 그리고, 상기 암호화 방식은, DES 알고리즘을 사용하는 암호화 방식을 사용하는 것이 바람직하다.

<29> 이하에서는 도면을 참조하여 본 발명을 보다 상세하게 설명한다.

<30> 본 발명은 도 1에 도시된 도면을 함께 참조하여 설명하되, 도 1에 도시한 부분과 동일한 부분에 대해서는 동일한 참조부호를 부여하여 인용한다.

<31> 도 4는 본 발명에 따른 RR 방법이 수행되는 과정을 설명하기 위한 신호 흐름도이다. 본 발명에서는 기본적으로 다음과 같은 상황을 가정한다. 즉, 이동노드(100)와 홈에이전트(150)사이에 안전한 채널(secure channel) 존재하고, 홈에이전트(150)와 대응노드(200) 사이에는 Diffie-Hellman 키교환을 위한 공개된 값 p,q 가 있다고 가정한다.

<32> 이러한 상황에서, 먼저 이동노드(100)는 홈에이전트(150)에게 HoTI(Home Test Init) 패킷을 전송하고(S400), 대응노드(200)에는 CoTI(Care of Test Init) 패킷을 전송한다(S420). 이동노드(100)가 홈에이전트(150)에 전송하는 HoTI 패킷 에는 다음과 같은 정보가 포함된다.

<33> ● HoTI:

<34> Source = home address

<35> Destination address = correspondent address

<36> Parameter : Home Init Cookie

<37> 또한, 이동노드(100)가 대응노드(200)에 전송하는 CoTI 패킷에는 다음과 같은 정보가 포함된다.

<38> ● CoTI:

<39> Source = care-of address

<40> Destination address = correspondent address

<41> Parameter : Care-of Init Cookie

<42> 홈에이전트(150)는 수신한 HoTI 패킷에 임의의 비밀키 및 공개된 값을 사용하여 산출한 키 정보를 HoTI 패킷에 포함시켜 대응노드(200)에 전송한다(S420). 이때, 키정보는 HoTI 패킷의 모바일 옵션(Mobile Options) 필드에 부가될 수 있다. 이러한 방식에 의해, 공개된 값 등으로 산출된 키 정보만이 전송되며, 네트워크상에서 자신의 비밀키는 공개되지 않는다.

<43> 대응노드(200)는 홈에이전트(150)가 전송한 HoTI 패킷에 대한 응답으로 HoT 패킷을 전송한다(S430). 이때, 전송되는 HoT 패킷에는 대응노드(200)가 공개된 값 및 임의의 비밀키로 산출된 키 정보과 포함된다. 키정보는 HoT 패킷의 모바일 옵션(Mobile Options) 필드에 부가

될 수 있으며, 이러한 방식에 의해, 홈에이전트(150)와 대응노드(200)는 키정보를 교환하여, 서로 공유된 비밀키를 가지게 된다.

<44> 홈에이전트(150)와 대응노드(200)과의 키교환을 위해서는 DH(Diffie-Hellman) 키교환 방법이 사용 가능하다. DH 키교환 알고리즘은 두개의 통신 노드가 공개적으로 오픈된 네트워크에서 통신할 때, 둘만의 비밀키를 공유할 수 있도록 하는 방법이다

<45> DH 키교환 방법은 1976년에 Diffie와 Hellman에 의해 개발되었고, 지침이 되는 논문 "New Directions in Cryptography"에서 발표되어 있다. 이 방법은 두개의 통신 노드 사이에서 사전에 어떠한 비밀교환 없이 안전하지 않은 매체상에서 공통의 비밀키를 생성할 수 있게 한다. DH 키교환 방법에서는, 두개의 시스템 파라미터 p와 q를 갖는데, 이들은 모두 공개되고 시스템 안의 모든 사용자들에 의해 사용될 수 있다. 파라미터 p는 소수이고, 일반적으로 생성자(generator)로 불리는 파라미터 q는 p보다 작은 정수이며, q는 그 자신이 어떤 횟수만큼 소수 p의 법으로 곱해질 때 1부터 p-1까지의 모든 요소들을 생성할 수 있다. 이러한 파라미터를 사용하여 홈에이전트(150)와 대응노드(200)는 다음과 같은 과정에 의해 공통의 비밀키를 생성하게 된다.

<46> 첫 번째로, 홈에이전트(150)는 랜덤한 비밀키 a를 생성하고 , 대응노드(200)는 랜덤한 비밀키 b를 생성한다. 그리고 나서 파라미터 p, q 및 비밀키들을 이용해서 다음의 수식에 의해 공개키들을 만든다.

<47> 【수학식 1】 $Y_a = q^a \bmod p$

<48> $Y_b = q^b \bmod p$

<49> 여기서, Y_a는 홈에이전트(150)의 공개키이고, Y_b 는 대응노드(200)의 공개키이다. 공개키 생성이 끝나면 서로 공개키를 교환한다. 공개키가 교환되면, 홈에이전트(150)와 대응노드(200)는 다음의 수식에 의해 공통의 비밀키 K 를 생성할 수 있게 된다.

<50> 【수학식 2】 $K_a = (Y_b)^a \bmod p$

<51> $K_a = (Y_a)^b \bmod p$

<52> $K_a = K_b = K$ 가 되므로, 홈에이전트(150)와 대응노드(200)는 공통의 비밀키 K 를 갖게 되며, 다른 노드들은 비밀키를 유추할 수 없다.

<53> 한편, 대응노드(200)는 홈에이전트(150)와 키정보 교환으로 생성한 비밀키를 사용하여 CoT 패킷을 암호화하여 이동노드(100)에 전송한다. 이동노드(100)는 홈에이전트(150)로부터 받은 비밀키를 사용하여, 대응노드(200)로부터 수신한 암호화된 CoT 패킷을 복호화할 수 있다.

<54> CoT 패킷을 암호화에는 여러가지 암호화방식이 사용가능하다. 이 경우, Mobile IPv6의 가장 큰 특징이면서 고려되어야 할 사항은, 이동노드(100)의 이동시, 어떠한 처리과정도 최대한 빠르고 간편한 알고리즘이 적용되어, 이동노드(100)의 통신 연결이 끊기지 않도록 하는 것이다.

<55> 이를 위해 본 발명에서는, CoT 패킷의 암호화에는 DES(Data Encryption Standard) 알고리즘을 사용한다. DES 알고리즘은 대칭키 블럭 알고리즘으로서, 개인키를 사용하여 데이터를 암호화하는 방법으로서 널리 사용되는 알고리즘이다. DES 알고리즘을 사용하여, 네트워크상의 데이터를 보호하고자 할 때, 통신노드는 암호화와 복호화에 사용되는 공유의 비밀키를 알고

있어야 한다. DES 알고리즘은, 각 64 비트 데이터 블록에, 56 비트 길이의 키를 이용하여, 16 번의 연산을 거쳐, 다시 64 비트의 암호문을 만들어 낸다.

<56> DES 알고리즘에서는, 72,000,000,000,000,000 (72천조)개 이상의 암호 키가 사용되는 것이 가능하다. 주어진 각 메시지를 위한 키는, 이렇게 막대한 양의 키 중에서 무작위로 선택된다. 다른 개인키 암호화 방법과 마찬가지로, 송신자와 수신자 둘 모두는 동일한 개인키를 알고, 사용해야 하는데, 본 발명에서는 홈에이전트(150)와 대응노드(200)간의 키정보 교환을 통해 생성한 비밀키를 사용한다. 사용환경에 따라서는 세개의 키가 잇달아 적용되는 "트리플 DES" 의 사용도 고려될 수 있다.

<57> 한편, 도 4의 RR 방법을 정리하면, 도 5에 도시한 바와 같이 된다. 도 4 및 도 5에서 도시한 과정에 의해 , 비밀키를 가진 이동노드(100)만이 대응노드(200)가 전송한 암호화된 CoT 패킷을 복호화할 수 있으므로, 중간자 공격을 배제하여, RR 과정의 안전성을 향상시킬 수 있으며, 이를 통해 이동노드(100)에 대한 인증도 동시에 가능하다. 또한, 키교환이 이동노드(100)와 대응노드(200)사이가 아닌, 홈에이전트(150)와 대응노드(200)사이에 이루어지므로 보다 안전성이 향상된다.

【발명의 효과】

<58> 이상 설명한 바와 같이, 본 발명에 따르면, 홈에이전트와 대응노드사이에 공개키를 사용하여 비밀키를 생성하고, 생성한 비밀키를 사용하여 대응노드에서 이동노드에 전송하는 패킷을 암호화하고, 암호화된 패킷을 비밀키를 사용하여 복호화 과정을 수행함으로써, 중간자 공격을 배제할 수 있다. 이에 의해, RR 과정의 안정성이 향상된다.

<59> 또한, 이상에서는 본 발명의 바람직한 실시예에 대하여 도시하고 설명하였지만, 본 발명은 상술한 특정의 실시예에 한정되지 아니하며, 청구범위에서 청구하는 본 발명의 요지를 벗어남이 없이 당해 발명이 속하는 기술분야에서 통상의 지식을 가진자에 의해 다양한 변형실시가 가능한 것은 물론이고, 이러한 변형실시들은 본 발명의 기술적 사상이나 전망으로부터 개별적으로 이해되어져서는 안될 것이다.

【특허청구범위】

【청구항 1】

이동노드, 홈에이전트, 및 대응노드간의 RR(Return Routability) 방법에 있어서,

상기 이동노드가 상기 홈에이전트에 HoTI 패킷을 전송하고, 상기 대응노드에 CoTI 패킷을 전송하는 단계;

상기 홈에이전트가 소정의 방식에 의해 생성한 제1 키 정보를 포함하는 HoTI 패킷을 상기 대응노드에 전송하는 단계;

상기 대응노드가 상기 소정의 방식에 의해 생성한 제2 키 정보를 포함하는 HoT 패킷을 상기 홈에이전트에 전송하고, 상기 제1 키 정보로부터 상기 소정의 방식에 의해 생성한 비밀키를 사용하여 암호화한 CoT 패킷을 상기 이동노드에 전송하는 단계;

상기 홈에이전트가 수신한 상기 HoT 패킷으로부터 상기 소정의 방식을 사용하여 생성한 상기 비밀키를 상기 이동노드에 전송하는 단계; 및

상기 이동노드가 수신한 상기 비밀키를 사용하여, 수신한 상기 암호화된 CoT 패킷을 복호화하는 단계;를 포함하는 것을 특징으로 하는 RR 방법.

【청구항 2】

제1항에 있어서,

상기 소정의 방식은, 공개된 파라미터 및 임의의 비밀키를 사용하는 Diffie-Hallman 키 교환 방식인 것을 특징으로 하는 RR 방법.

【청구항 3】

제1항에 있어서,

상기 제1 키 정보는, 상기 HoTI 패킷의 모바일 옵션(Mobile Options) 필드에 첨가되는 것을 특징으로 하는 RR 방법.

【청구항 4】

제1항에 있어서,

상기 제2 키 정보는, 상기 HoT 패킷의 모바일 옵션(Mobile Options) 필드에 첨가되는 것을 특징으로 하는 RR 방법.

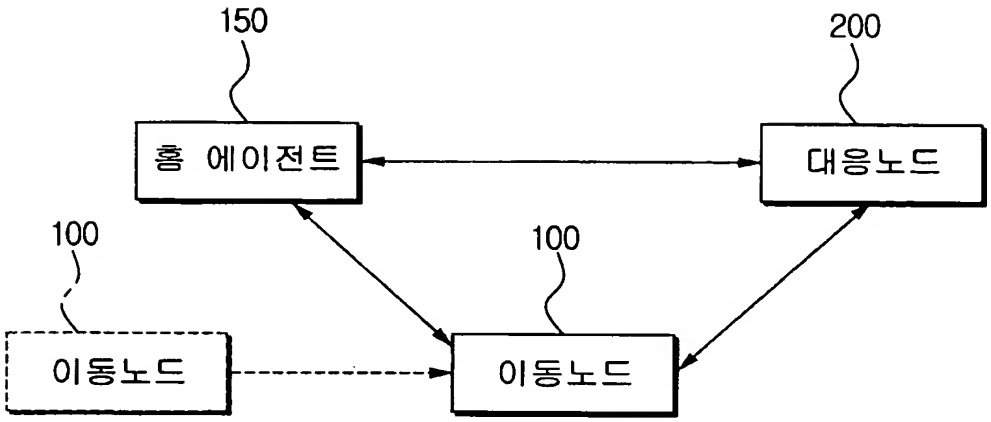
【청구항 5】

제1항에 있어서,

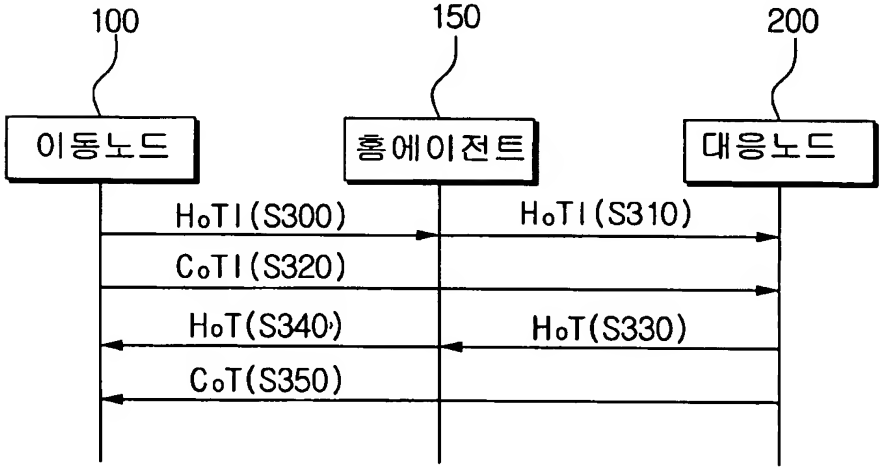
상기 암호화 방식은, DES 알고리즘을 사용하는 암호화 방식인 것을 특징으로 하는 RR 방법.

【도면】

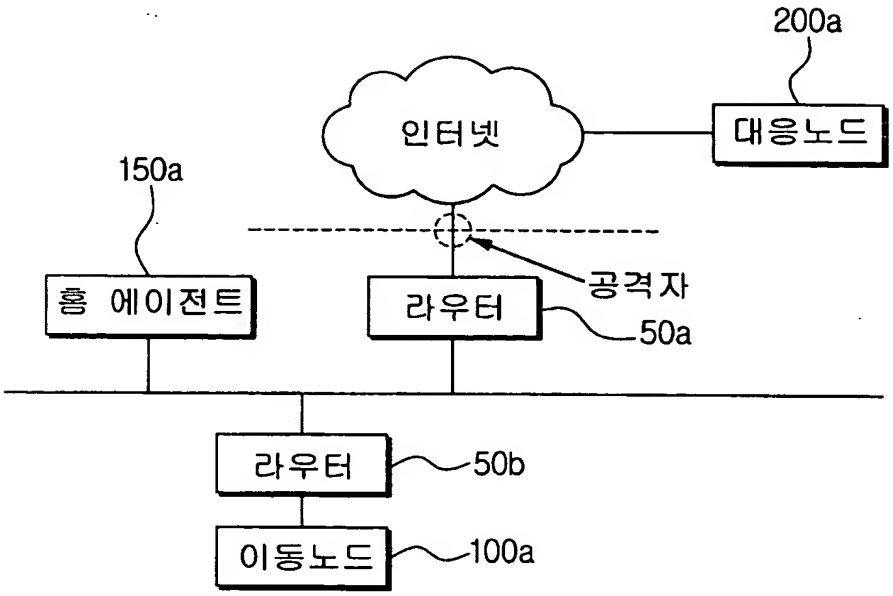
【도 1】


150
200
홈 에이전트
대응노드
100
100
이동노드
이동노드

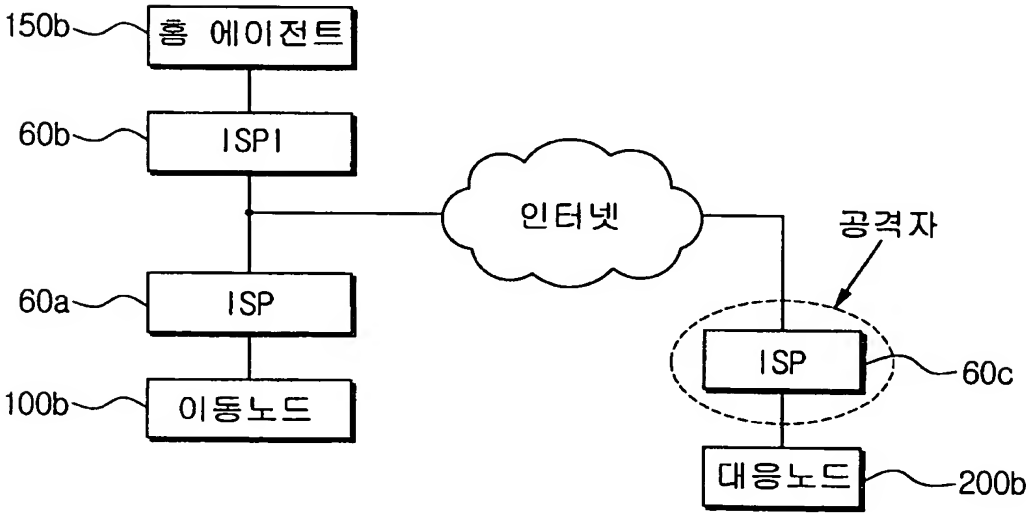
【도 2】


100
150
200
이동노드
홈에이전트
대응노드
HoTI(S300)
HoTI(S310)
CoTI(S320)
HoT(S340)
HoT(S330)
CoT(S350)

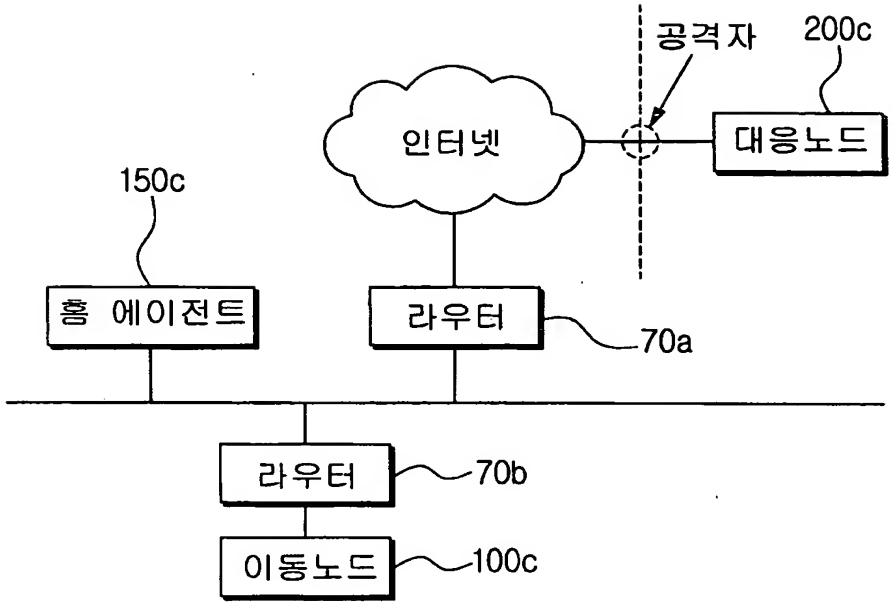
【도 3a】


200a
인터넷
대응노드
150a
홈 에이전트
라우터
공격자
50a
라우터
50b
이동노드
100a

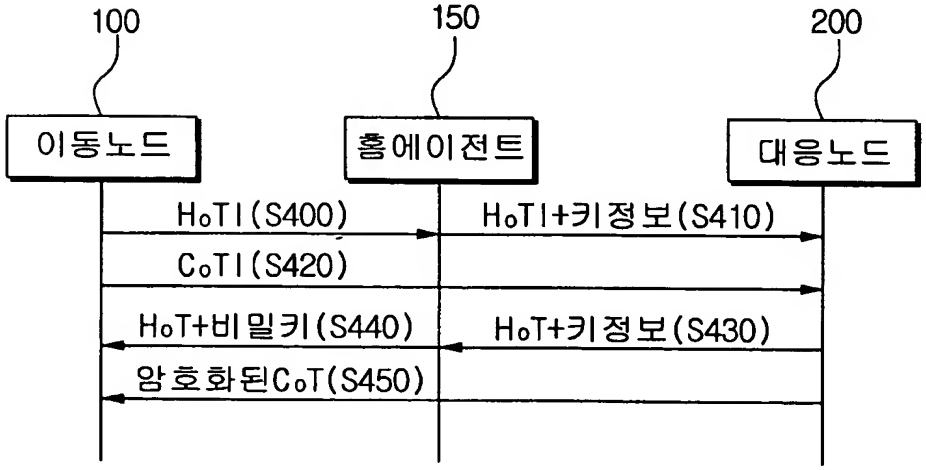
【도 3b】


150b
홈 에이전트
60b
ISP1
인터넷
공격자
60a
ISP
ISP
60c
100b
이동노드
대응노드
200b

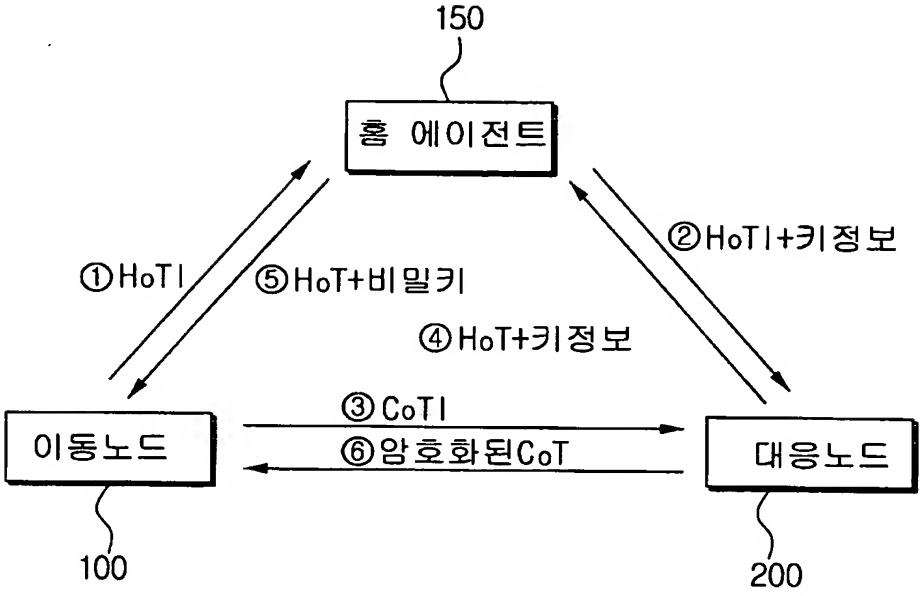
【도 3c】


공격자
200c
인터넷
대응노드
150c
홈 에이전트
라우터
70a
라우터
70b
이동노드
100c

【도 4】


100
150
200
이동노드
홈에이전트
대응노드
HoTI(S400)
HoTI+키정보(S410)
CoTI(S420)
HoT+비밀키(S440)
HoT+키정보(S430)
암호화된CoT(S450)

【도 5】


150
홈 에이전트
①HoTI
⑤HoT+비밀키
②HoTI+키정보
④HoT+키정보
③CoTI
⑥암호화된CoT
이동노드
대응노드
100
200